APPENDIX G

CONFIGURATION MANAGEMENT

AND

SOFTWARE MANAGEMENT PLAN

FOR THE

SECURE VIDEO TELECONFERENCING SYSTEM (SVTS)

TABLE OF CONTENTS

## SECTION 1

## INTRODUCTION

1.1 **Background**. The Executive Branch Network Engineering Branch of the Defense Information Systems Agency (DISA) is the designated Program Management Office (PMO) for the Secure Video Teleconferencing System (SVTS). As Program Manager, the Executive Branch Network Engineering Branch will over see the technical integrity and security of the SVTS. The SVTS Network Certification Working Group (NCWG) will ensure that all proposed system changes meet the stringent security requirements of the SVTS. Any changes to the system must ensure the continuing integrity and security of SVTS capabilities. This will be accomplished through strict adherence to the Configuration Management (CM) procedures set forth in this plan.

1.2 **Purpose**. This plan establishes the following CM policies and procedures:

a. The organizational structure, responsibilities, and relationships involved in the CM process.

b. The process for expanding the system to respond to changing user requirements by defining procedures for the processing of change proposals.

c. The procedures by which a contractor implements changes and modifications to the SVTS hardware and software, and by which commercial off-the-shelf (COTS) software is integrated into the system. The objective is to establish a repeatable process for development and maintenance of the SVTS hardware and software.

1.3 **Scope**.

a. This document provides Configuration Management (CM) and Software Management procedures which ensure that any changes to the existing system will support the continuing integrity and security for SVTS capabilities. The plan establishes a process for expanding and changing the system to respond to changing user requirements by defining procedures for processing change proposals. Further, the plan identifies the organizational structure, responsibilities, and relationships involved in the CM process.

b. This plan defines software lifecycle management from the development of a task for a system change or the issuance of a Software Trouble Report (STR) to the installation and postrelease testing of a new release in the field. Software maintenance is also included. This plan addresses the specific steps and verifications that will be performed during the software lifecycle.

## 1.4 **Applicability and Authority**.

a. This SVTS Configuration Management and Software Management Plan is a tailored or modified version of the Military Standard for Configuration management (MIL-STD-973), the Military Standard for Defense System Software Development and Documentation (MIL-STD-498), and the SVTS Network Security Manual. However, in the event of a conflict between this plan and the references cited above, the text of the references takes precedence. The contractor shall bring all discrepancies to the attention of the Government.

b. The provisions of this plan apply to all activities involved in the development, implementation, operation, and maintenance of the SVTS.

c. The document will be used as a guideline for contractors and the Government and its representatives for the development and installation of hardware and application software and the integration and installation of COTS software. Each step in the software life-cycle for a software change is described. The section on Software Management will be used to manage the development effort or maintenance effort to implement software changes.

(1) The names and locations of files and directories, the format and content of the Software Version Description (SVD) Document, and procedures for the production of formal tape builds, running check sums, downloading files and other software development/ operating procedures are covered in the SVTS Programmer's Maintenance Manual and the SVTS Software Installation Manual.

## SECTION 2

## CONFIGURATION MANAGEMENT

2.1 **CM ORGANIZATION AND RESPONSIBILITIES**. The organizational structure for Government CM is depicted in figure 2-1. Specific responsibilities of organizations involved in the CM process are identified in the following subsections.

2.1.1. CM Responsibilities.

a. Configuration Control and Approval.

(1) Situation Support Working Group. The Situation Support Working Group (SSWG) will function as the Configuration Control Board (CCB) and will serve as the body that controls changes to the baseline system. The SSWG will be comprised of individuals from the user community, the National Security Agency (NSA), and the PMO. The SSWG Chairman or his designated representative will be the approving authority for all proposed changes. Specific responsibilities of the SSWG are as follows:

(a) Provide management focus for all proposed changes during the evaluation and approval process.

(b) Establish priorities and schedules as necessary to allow for a smooth integration of any proposed changes.

(c) Provide management guidance and direction relative to funding and resource thresholds for any proposed change.

b. Configuration Management. The SVTS Program Manager will be the principal Configuration Manager. Proposed changes will be submitted to the Program Manager for coordination of the technical and security evaluations. The evaluation and recommendation process will occur prior to submission of the change proposal to the SSWG for approval or disapproval. Specific Program Manager responsibilities include, but are not limited to items 1-10. Contractor assistance may be required to carry out the responsibilities.

(1) As necessary, designate a Principal Action Officer (PAO) to evaluate impacts of the proposed change, to assess completeness and to ensure timely processing.

(2) As necessary, designate technical representatives to perform an evaluation of the technical impacts of a proposed change (see paragraph D.).

(3) Prepare a prioritized schedule of change processing actions.

# SSWG

(Configuration

Control and Approval)

Program Manager

(Configuration

Management)

Principal
Action Officer
(Technical Evaluation
and Processing)

Technical
Representative
(Technical Evaluation)

Figure **2-1** Government **CM** Organization

(4) Forward, concurrent with technical review by the PAO, copies of the change proposal to interested agencies for review (including the technical representative for preliminary review prior to the convened SSWG meeting).

(5) Schedule the SSWG meetings and forward to SSWG members the meeting notification, meeting agenda, and the change proposal(s).

(6) Record and publish the SSWG actions and provide copies to all interested parties expected to be impacted by the SSWG decision.

(7) Determine that an approved change has been properly tested and implemented.

(8) Establish and maintain a CM library of baseline documentation, drawings, and technical manuals (see section 2.2.2); ensure that the approved change has been incorporated into the baseline documentation.

(9) Implement a status accounting system (see section 2.4) and monitor the status of all change actions.

(10) Ensure adherence to and periodic reviews and update of this CM plan.

c. Change Evaluation and Processing. The PAO will be a representative from the PMO. As directed by the Configuration Manager, the PAO will have primary responsibility for technical evaluation and processing of all change proposals. Specific Configuration Manager responsibilities include, but are not limited to items 1-3. Contractor assistance may be required to carry out the responsibilities.

(1) Ensure completeness and inclusion of all supporting technical documentation in the change proposal package, including changes to configuration drawings, interface documents, and nomenclature for interfacing Configuration Items (CIs), affected document identification, change pages for affected specifications, Commercial Off-the-Shelf (COTS) descriptions, and software version descriptions or computer program listings.

(2) Review the change proposal and evaluate all impacts on the configuration items with which the proposed change will interface. At a minimum the review should include consideration of the following items:

(a) Security impacts.

(b) Cost of the change to the Government, contractor, or user.

(c) Schedule impacts.

(d) Logistics requirements.

(e) Maintenance support.

(f) Interface impacts.

(g) Skill, manning, training, and man-machine interface requirements.

(3) Based on the technical evaluation and recommendations of other interested agencies, prepare and present to the SSWG a briefing that summarizes recommendation, including the positions of various agency representatives expected to be impacted by the proposed change.

d. Change Technical Evaluation. As required, the Program Manager will assign government technical representatives to provide an evaluation of technical impacts of the proposed change. Contractor personnel may be required to assist in this evaluation. The government technical representative will assist in the review process and in determining the appropriate action for change proposals brought before the NCWG. The government technical representative and contractor personnel who assist in these efforts must be knowledgeable in the areas of security, logistics, training, and maintenance relating to the hardware or software environment. Specific responsibilities include, but are not limited to, the following:

(1) Review the change proposal prior to the schedule SSWG meeting.

(2) Advise the convened SSWG on the technical impacts of the proposed change.

2.1.2 CM Relationship to Other Organizations

a. Node/Hub Configuration Control Management. The Node/Hub Information System Security Officer (NISSO/HISSO) will serve as the focal point for CM and control of user-proposed changes to the baseline system. The NISSO/HISSO will ensure that

all change proposals are submitted in the proper format to the Program Manager for formal processing, and will ensure clarity, completeness of technical content, and adequacy of impact statements.

b. Network Certification Working Group. As the group responsible for certification and recertification of the SVTS, the NCWG will be the final authority to determine if an approved change has been correctly implemented. Close liaison will be maintained with the SVTS Network Security Officer and the Program Manager in the coordination, testing, and recertification process.

## 2.2 CONFIGURATION IDENTIFICATION.

2.2.1 Configuration Items (CI). The current configuration identification represents the baseline for the CIs for hardware, software, and facilities. CIs consist of (1) segments, that refer to the node, hub, and related telecommunications; and (2) elements, that refer to hardware and software modules that make up the segments. CIs will be used primarily for CM of the system and for identifying specific site configurations.

2.2.2 Baseline Documentation. All Government-approved baseline documentation for each CI will be placed under configuration control. These documents will be subject to modification and update as changes are approved. In all cases, references to and changes in the baseline documentation will be made to the current version of each document. For each new software release and hardware installation, the contractor shall update the CM baseline documentation and generate change pages. Baseline documentation for the SVTS segments and elements are contained in the following documents:

a. Hardware and facilities documentation:

(1) Engineering and Installation Plans

(2) Government-Furnished Equipment/Government-Furnished Manuals.

(3) COTS equipment descriptions

(4) External ports interface documents

b. Software documentation:

(1) Software Installation Manual

(2) Functional Specification

(3) System Interface Specifications

(4) Software Program Specifications for the HCP, NCP, UCT, and Data and Systems Utilities

(5) Software Program Maintenance Manual

(6) Network Controller Manual

(7) System Controller Manual

(8) Technical Controller Manual

(9) Hub Operations Manual

(10) Node Operations Manual

(11) Node Training Manual

(12) Hub Training Manual

(13) SVTS Technical Manual

(14) Program Documentation for the SVTS Support System

(15) Operation and Maintenance Manual

## 2.3 CONFIGURATION CONTROL.

2.3.1 Change Processing. Configuration control of the change process will ensure that the full impact of proposed changes to a CI is considered before change approval is given. The change process is depicted in figure 2-2 and is described in items a-f. The contractor may be required to assist in each of these items:

**Prepare Change Proposal**
**User**
nitiate **CM** Process;**Assign** Priority
**Program Manager**

AsseSS **Evaluate** Evaluate **Other**
**Complet ness;**
**ampac** Security **Impacts** Technical Impacts **Evaluation**
**Evaluate I ts**

Principal Action Officer NCWG **Technical** Rep **L;ontractor**

Consolidate
Recommendations

Program Manager
Archive; Notify
Originator
IIWG Program Manager

Notify

Interested Parties

P ger

Implement/Modify
Change and Test
User, Conlraclor
**Verify**
**Change**

P er

**C;@rt ify**

**Sy@t4a@**

**NCWG**

Figure **2-2**

Change Process Flow Diagram

a. When the need for a change becomes apparent, a change proposal may be initiated by the user, the development contractor, the PMO, or other agencies involved in SVTS development and implementation.

b. Each change proposal will be accompanied by supporting documentation and a Specification Change Notice (SCN) (CDRL A011) if changes to a specification are required.

c. The change proposal will be forwarded to the Program Manager for preliminary review to ensure completeness of documentation. The Program Manager will distribute the change proposal to the assigned PAO, the SSWG, technical representatives and any other interested parties for review and recommendations. These recommendations will be evaluated and coordinated by the Program Manager and forwarded to the SSWG for final approval or disapproval.

d. The Program Manager will initiate the change implementation process if the change proposal has been approved, or archive the change proposal if it has not been approved. The change may be implemented by the user, the PMO, the development contractor, or other agencies involved in SVTS implementation through the standard acquisition process or COTS acquisition.

e. The Program Manager will determine, through on-site inspections or evaluation of test reports, that the change has been correctly implemented.

f. As required, the SVTS will be certified by the NCWG for continued operations.

2.3.2 Reporting Documentation. The change proposal will provide extensive documentation to support and justify the request. It will contain a compilation of the information needed by the decision making organizations and will detail the proposal's impact on the approved baseline, cost, schedule, interfaces, security, logistics, maintenance, and training. The format for the change proposal is provided in annex A. An impact analysis checklist is provided in annex B. Each change proposal will include an ***SCN*** for each specification recommended for change. The SCN will identify a proposed change to a specification, provide a record of the change, and transmit the change pages.

2.4 **CONFIGURATION STATUS ACCOUNTING**. The Program Manager will maintain the records and compile the reports necessary to manage

the configuration effectively. Status accounting will provide traceability of the approved changes to their configuration, baseline. Records will include the technical documentation that defines the configuration of a CI, the status of proposed changes to that configuration, and implementation status of the approved changes for each CI.

2.4.1 CM Library. The Program Manager is responsible for maintaining a library of CM baseline documentation to support status accounting reports for each CI. The contractor shall assist in this effort at the direction of the program manager. This library will contain the technical data necessary to maintain these reports. The Program Manager will have the responsibility to ensure that status accounting records continue to reflect the latest configuration of any of the delivered items. At a minimum, the CM Library will contain the following items:

a. Documents listed in section 2.2.2 and approved changes to the baseline documents.

b. All proposed changes.

c. The following list represents the type of data required for maintaining status accounting records of the SVTS and its cis:

(1) The specific nomenclature which identifies each configuration item.

((2) The title, CDRL number and revision, and issue date of each specification and drawing that is a part of the baseline for each configuration item.

(3(3) Identification of change proposal for that configuration item.

(4) Identification and implementation data for approved changes to the configuration item.

d. Status accounting records will be initiated upon receipt of a proposed change by the Program Manager and updated periodically throughout the approval, implementation, and certification cycle. Reports will be issued as necessary.

2.4.2 Site Configuration Inspection. Sites will be inspected periodically for conformance to the approved configuration for that site. No modification will be made to the baseline system

prior to approval of the SSWG. Any modification will be made at

individual sites that has not been approved by the CMWG will be reported to the Network Security Officer as a violation of system security. This action may result in loss of site or system certification for continued operations.

2.5 **CONTRACTOR=S CONFIGURATION MANAGEMENT PLAN (CDRL C001)**. The Configuration Management Plan shall provide detailed information about how the contractor will fulfill his/her CM responsibilities, with particular emphasis on the work described above in this section (Section 2) of this Configuration Management & Software Management Plan. The contractor=s Configuration Management Plan shall include the contractor=s CM organization structure, personnel involved with the CM effort, procedures for change proposals, organization and procedures for the CM library, the system and procedures for CM status accounting, procedures for technical evaluations, update procedures for changes to baseline documentation, and procedures for configuration control. In preparing the Configuration Management Plan, the contractor should confer with the PMO to determine the extent of contractor involvement that the PMO anticipates will be required in the various aspects of the CM effort.

## Section 3.0

## SOFTWARE MANAGEMENT

3.1 **Section Introduction and overview**. Section 3 addresses software management and provides the detailed procedures and processes which a contractor shall use when implementing software changes to the SVTS software.

a. The SVTS software is currently written in DEC VAX PASCAL, BORLAND TURBO PASCAL the knowledge-based engineering language GENSYM G2, and DEC DCL operating system-level command interpreter (script) language. Additionally, the COTS software packages used in the system are listed in paragraph 2 of Appendix C. Total SVTS software consists of approximately 200K source lines of code distributed amongst multiple platforms and applications.

b. The contractor shall be responsible for performing engineering changes as tasked; for maintaining the developed system software; for providing the latest versions of the operating system software and the latest version of all COTS software; and for maintaining operating system software and all COTS software.

3.2 **Contractor=s Software Development Plan (CDRL S001)**. The Software Development Plan shall include the contractor's software management organizational structure, personnel, installation and maintenance procedures, software development library organization and procedures, software development files, and handling of project media. The plans and procedures for ensuring that the formal release version is error-free and exactly the same as the version tested during the test phase shall be included. The plan shall include controls for the secure movement of formal tape/disk builds to the field.

The contractor shall use the NSA-approved and Government furnished CHECKSUM utility software in the contractor's plans for software development to certify that the software modules placed in a formal tape/disk build are exactly the same as those installed in the field. (CHECKSUM is a SVTS-unique computer program that generates a unique number for all executable modules, data files, and operating system-level command interpreter (script) language files in a release. It is based on a bit-by-bit checking on each file. When run against the fielded software release CHECKSUM
display which files, if any, have changed from the build tape/disk.)

3.3 **New Tasks**. The contractor will receive task orders from the Government to perform software upgrades and changes or to perform investigations or studies which could eventually lead to a software change. An investigative task is a mechanism to provide the Government with alternative methods of changing or upgrading a current function of the system. The result of a task will be a set of options with estimated implementation costs.

3.3.1 Government Responsibilities.

a. The Government will provide the contractor with tasking to perform new work. This new tasking or the Software Trouble Report (STR) described in section 3.4 is the basis for software corrections. New taskings are also the basis for investigations for potential changes.

b. The Government will witness all tests, formal build processes, and CHECKSUM generations and for verifying CHECKSUM reporting in the field.

c. The Government will verify sealed tape/disk releases have not been tampered with. The Government will verify software has been properly installed.

d. The Government will review and approve design and in-progress reviews, all schedules, and all delivered documentation including test plans, test descriptions, and test reports.

e. The Government will determine the criticality of problems identified in STRS. The Government will determine when to release software and which task orders and STRs to place in each release.

3.3.2 Contractor Responsibilities.

a. The contractor shall perform no software development nor will the contractor conduct any software investigations without a task order from the Government. No coding shall be initiated for a task until the Government has approved the Preliminary Software Design Document. Government tasking is required for prototype efforts. The contractor is not prohibited from performing examination and review of the existing software code without a task order in order to perform an analysis of the scope of a problem and/or the impact of a potential software change to the existing system.

b. The contractor shall do software maintenance.

c. Except in the case of emergency STRS, the contractor shall do no software coding until the Government has approved the Preliminary Design Document.

3.3.2.1 Subtask/STR Form and SDF. The contractor shall be responsible for maintaining a Software Development File (SDF) in conformance with MIL-STD-498. The SDF shall contain the sub- task/STR forms and programmer notes for each subtask/STR. The SDF will include the subtask/STR form, design notes, information documentation updates, and test plans. The SDF shall include records of decisions made, supporting information on which decisions were based, and the conclusions reached.

3.4 **Software Maintenance**.

3.4.1 Introduction. The contractor shall provide 24 hours per day, seven days per week, on-call software maintenance support for all SVTS software including in house developed code, the operat- ing system software, and all COTS software listed in paragraph 2 of Appendix C to the statement of work. The contractor shall provide software support to correct any software related malfunc-tions, design errors, logic errors, or implementation flaws. The contractor shall keep up to date with published deficiencies, problems, solutions, patches and workarounds for all SVTS COTS software, to include the SVTS operating system and all other COTS software in use in the SVTS. The contractor shall keep the government apprised of this information and shall indicate which items may impact SVTS operations. The government may require selected items to be included in the Software Trouble Report (STR) process.

3.4.2 Overview. This subsection on software maintenance describes the procedures or steps involved in the reporting, in- vestigation and correction of possible software problems in SVTS developed code, the operating system software, to include script files, the expert system and its related software, and all system software including COTS software. Also included in this subsec- tion are the steps to be followed for maintaining COTS software and the operating system software.

3.4.3 Software Trouble Reports. Upon discovering a possible software problem, the person (Government or contractor) making the discovery will fill out a Software Trouble Report or STR (CDRL S010) and submit it to the contractor's Configuration manager. The ori- ginator of the STR will fill out, as a minimum, his name and phone number, the date, the title of the STR, and the trouble descrip- tion. The contractor shall fill out each entry on the STR form.

The STR provides an internal procedure for reporting and tracking software or software related problems. The cost, impacts, and all possible solutions are documented on the STR form. The STR will include impact in estimated Source Lines of Code (SLOC) to be changed and staff-hours to complete. Some solutions may require modification, removal and/or addition of lines of code.

3.4.4 Managing Emergency Fixes. The contractor's Configuration Manager shall immediately log all reported STRs to allow tracking of all phases of software related updates. Upon notification of a
potential software problem, the contractor shall immediately noti- fy the Government of the problem. The Government will determine whether the correction of a software problem will be installed in the system immediately or as part of a future software release. The Government will determine whether the problem identified in the STR has resulted in or could result in a failure which criti- cally impacts SVTS operations (e.g., problems which can cause total system failure, failure of system functional capabilities, failure impacting upon system security, or failure of system con- trol elements, which preclude use of the system, functional capa- bilities, or system controls). If the Government determines that the problem correction is critical to SVTS operations, then the contractor shall determine a solution, modify and test the code, and install the corrected code in the field following the release procedures described in section 3.9.1.2 within 48 hours. In the case of failures which impact system security, the contractor shall implement the change immediately. In no case shall the contractor install software changes in the field without Government approval.

3.4.5 Software Implementation.

a. If the Government determines that a reported problem does not present a condition which would critically impact upon SVTS operations, then the contractor shall provide the Government a complete analysis of the STR within ten working days after the problem occurred. If the problem is found to be hardware, it will be so noted on the STR and turned over to maintenance for correc- tion. If the problem is found to be software it will be turned over to the contractor's software development team for resolution.

b. The contractor shall determine impacts, determine possible solutions, and recommend a solution to the Government (this is the Preliminary Software Design Document of section 3.6.1). Government approval is required before a software solution can be implemented. If the proposed solution is not ap-

approved by the Government, the STR will be returned to the contractor for further evaluation. The approval stage will continue until a solution is agreed to by both the Government and the contractor.

c. Upon Government approval the contractor shall implement the solution, verify the solution with Government witnessing using the test requirements of section 3.8 with Government witnessing, and capture the release as described in section 3.9.

3.4.6 Software Development Files. See subsection 3.3.2.1.

3.4.7 Software Releases. The Government will determine whether the contractor will install the fix as part of a future scheduled release for enhancements, or to install it by itself or as part of a maintenance release. The Government may require the contractor to install up to three (3) software releases for maintenance per year (this is over and beyond emergency releases to fix critical problems).

3.4.8 Operating System and COTS Software. The contractor shall be responsible for maintaining the operating system software and COTS software as described in section 3.1.1.3.3 in the statement of work.

3.5 **Software Designs**. The contractor shall be responsible for making preliminary and detailed designs for all software changes to be made, including changes required by Government task orders and statements of work, and those changes required in order to implement fixes to problems documented in STRS.

3.5.1 Preliminary Software Design. The contractor shall develop a Preliminary Software Design Document using CDRL S002 for all software changes which will be required as the result of a Government task order or that will be required in order to correct a software problem which has been identified in a STR. The preliminary software design will include, but not be limited to, a high-level description of the design approach, alternatives considered, and the reason for selecting the recommended approach, and the schedule for designing, coding, testing, and installing the change. The design shall include modules to be changed, their function and reason for change, interfaces to hardware and other software components, flow diagrams, and draft copies of proposed human interface screens which would be modified or changed.

3.5.2 Detailed Software Design. After completion of the

Software Design Review and after the contractor has satisfactorily completed all action items which resulted from the review, and upon Government approval of the Preliminary Software Design Docu- ment, the contractor shall develop a Software Detailed Design Document for all new task orders for software changes and
for all software changes required to correct problems identified in a STR. The detailed design document will be used to verify completeness, consistency, and traceability to requirements and system design specifications and budgets. The draft detailed design document will be the basis from which the contractor shall develop code.

3.5.3 Designs for Emergency STRS. Emergency software problems as defined in section 3.4.4 shall be corrected immediately. The design approach shall be discussed orally with the Government, but the necessary design documents shall be provided within 45 calen- ndar days after the change has been installed in the field.

3.6 **Software Design Review and In-Progress Reviews**.

3.6.1 Software Design Review.

3.6.1.1 General. The contractor shall conduct a Software Design Review within one month of the start of a Government ordered task for a software enhancement or investigation/study. Software De- sign Reviews for correcting problems documented in STRs shall be conducted within 2.5 months prior to the Government scheduled release dates for the STR (except in the case of emergency STRs discussed in sections 3.5.3).

3.6.1.2 Software Enhancement/STR Software Design Review. A Software Design Review shall be conducted by the contractor for all software enhancements and for STR corrections. At the review the contractor shall discuss the status of the task/STR, the Pre- liminary Design Document, and other issues concerning the design and implementation of the task/STR.

3.6.1.3 Investigative Study Software Design Review. A Software Design Review shall be conducted within 21 calendar days from the start of a Government task order for an investigation or study. At this review the contractor shall present the status of the study, the contractor's approach for investigating the problem, impacts, alternatives, advantages/disadvantages, the schedule, the work remaining to be done, and any other issues pertinent to the conduct of the study.

3.6.1.4 Conduct of Software Design Reviews. An agenda and participant list for the Software Design Review will be established jointly by the contractor and the Government at least one week prior to the review. The Government will receive copies of the review package one week prior to the review. During the review, any specific areas of concern will be discussed by the Government and the contractor, and action items will be assigned. The contractor shall use CDRL A005 to prepare minutes of the review including the action item assignments and the schedule for completing the action items. A preliminary assessment of the potential cost and schedule impact will be included in each action item that affects the proposed design of a task. The minutes package shall be sent to the Government within one week after the review. Upon receipt of the completed action items, the Govern- ment will provide necessary direction to the contractor, including selection/deleletion of items for a given release and/or adjust- ments to the cost and schedule for a given release. The Govern- ment will approve the final minutes and the Government will distribute them. The contractor shall not commence detailed designs until the Government has approved the Preliminary Software Design.

3.6.2 In-Progress Reviews. In-Progress Reviews shall be conducted as specified in the Government issued task order, and as the need arises as mutually agreed to by the Government and the contractor.

3.7 **Software Coding**. Software coding shall be developed in accordance with the software design as specified in the Software Detailed Design Document (CDRL S002). If, while developing new code or modifying existing code, it is necessary to make design changes, the Software Design Document shall be updated to reflect the changes. No coding shall begin until the draft Software Detailed Design has been completed.

3.8 **Software Testing**.

3.8.1 Overview. The contractor will be responsible for verifying that all developed software is functioning properly by developing for Government approval and conducting with the Government as witness, various levels of individual functional and regression tests. The contractor shall be responsible for developing a test plan and a prerelease test, a post release test, and field test for each software release. The prerelease test shall include individual tests to test specific changes made as a result of a task order or STR and a system regression test which ensures the proper functioning and performance of the total system functions and services. The Post Release test shall

verify that the formal build software and the routines/procedures to automate the distribution of the software in the field, is functioning properly. Additionally, the contractor is strongly encouraged to conduct individual unit tests to verify the functionality of individual software units (computer programs and subroutines) as they are developed. All test plans and results shall be kept in the Software Development File (SDF). No alterations of the code will be made during any of the testing (except for unit testing) in order to insure the validity of the release. During testing
and upon Government approval, the contractor may modify a test plan, but a new plan must be written within 24 hours after the Government approval.

3.8.2 Software Test Plan. The contractor shall provide the Government a Software Test Plan that describes the integration and test strategy, identifies essential test resources required for
integration testing and establishes the schedule for such activities. The Software Test Plan format is described in CDRL S007.

3.8.3 Unit Testing. As the contractor develops code for a task unit (individual computer program or subroutine) or STR unit, he should develop and execute tests to verify the functionality of each unit. The contractor does not need Government approval for the individual unit tests, but the test codes, procedures, and results shall be kept in the SDF. Some of the unit tests which the contractor should consider conducting include, but are not limited to, the following:

a. Source Code Files:
Use a symbolic debugger or development of special test cases.

b. Screen Management Files: Software should be executed to display all modified or developed FMS screens.

c. Message Files:
The corresponding software unit which uses the messages defined in the Message file should be executed to verify the content and the correct function of the modified message.

d. Data Files:
Software which reads modified data files and modified software which read data files should be tested.

e. Script Files:
Modified/added command files and the software units which invoke

these command files should be executed to verify that they produce the desired results.

3.8.4 PreRelease Testing.

3.8.4.1 General. The contractor shall generate a prerelease build prior to conducting the prerelease tests.

a. This test build will incorporate all the changes to be included in the formal release, but it will not be formally promoted to the release library. The prerelease build shall be free of all compilation and link errors.

b. The prerelease tests shall include individual functional and regression tests (CDRL S008) and a system regression test (CDRL S008).

c. The Individual Functional/Regression test plans shall be included in the subtask/STR SDF folder. The prerelease tests will be witnessed and approved by the Government.

3.8.4.2 Individual Functional/Regression Tests.

3.8.4.2.1 General. The Individual Functional/Regression tests will be used to ensure the functional performance of the system and the SVTS services.

a. The contractor shall develop an Individual Functional/Regression test as part of the completion criteria for each subtask/STR form. The tests will isolate each change in the system and verify that changes conform to the functional and software design requirements. Functions likely to have been changed will be regression tested at this time to ensure that they still perform correctly.

b. During all tests, the contractor or a Government representative shall document any Individual Functional/Regression test failures on a comment form. The Government will have one week to provide comments to the contractor on the Individual Functional/Regression test failures. All Individual Functional/Regression tests which failed during testing shall be successfully retested with Government witnessing and approval prior to the System Regression test.

3.8.4.2.2 Description of Tests. Each test will verify a particular change from a system-wide perspective. The individual functional test will verify the direct results of a specific change, and the regression test will verify the indirect (e.g.,

the relationship of the added or changed unit to the rest of the system) results of each change. Each Individual Functional/Regression Test (CDRL S008) will include, but not be limited to, a task identifier, responsible engineer, brief description of problem and problem solution(s), test cases, step by step functional tests, regression tests, DE&I resources required, and time

to perform tests. The tests will be witnessed and approved by Government representatives.

3.8.4.3 System Regression Test.

3.8.4.3.1 General. The System Regression Test will be a set of system level tests that ensures the proper system functioning and performance of the total system functions and services. This test ensures that software modified in one module, does not adversely affect other software modules or the hardware/software interface.

3.8.4.3.2 Description of System Regression Test. The System Regression Test verifies the functionality of the entire SVTS system. The Government will witness and approve the test. This test shall follow only after a satisfactory retest (should any be required) of the Individual Functional/Regression tests. The System Regression Test will use the same test release software that is used for the Individual Functional/Regression tests. The System Regression Test format is described in CDRL S008. If a part of the System Regression Test does not work, the Government will decide as to which step to back up to, or, if necessary, to restart the test from the beginning.

3.8.4.4 Test Failures and Recovery for PreRelease Tests.

3.8.4.4.1 Detection/Correction Of Errors. A comment form will document all failures of an Individual Functional/Regression Test or System Regression Test. The Government will have one week to provide comments. Within 1 week after testing, the Government will determine whether a subtask/STR which failed testing should be removed from the release or corrected. If the Government directs the contractor to correct the failed software for the current release, the Government will determine which tests or portions of a test will need to be rerun in order to validate the change.

3.8.4.4.2 Recovery Procedure. The Government and the contractor will jointly resolve any problems that may develop because of a test failure. If the failure is caused by a hard-

ware problem, the contractor shall correct the problem. The Government will determine the point in the test plan at which testing will be resumed. If the cause of a subtask/STR failure is due to a software error and can be easily corrected, updates to the appropriate modules shall be made and a new test build generated. If the failure is due to a compilation or linking failure, a new compile and link will be performed to produce another test release. No partial compilations or links are acceptable for the test release. If a new test build is made, the Government will determine the point at which testing will be resumed.

3.8.4.4.3 Change or Removal of Subtask/STRs From the Release. If the failure cannot be easily corrected, the applicable subtask/STR may be removed from the release with Government approval. The contractor's Configuration Management (CM) will remove the failed module(s) from the promotion list. If a Subtask/STR is removed from the release, the System Regression Test, Post Release Test, and Field Test shall be updated accordingly. The Government will determine the point at which testing will be re-run.

3.8.5 Post-Release Testing.

3.8.5.1 General. After the prerelease software has been successfully tested, a formal build tape/disk will be generated which will incorporate all of the changes to be included in the Formal Release. The Formal Release shall be free of all compilation and link errors. A file comparison program, currently VMS DIFFERENCES, will be run to certify that the executable modules, data files and command files in the Formal Release are identical to the modules which were used in the Test Release.

3.8.5.2 Description of Test. The contractor shall furnish for Government review a Post Release Test Plan. After a successful compilation and linkage, a Formal Release will be installed in the DE&I facility. The Post Release Test will validate the routines/procedures to automate the distribution of the software in the field, and the basic functionality of the Formal Release. The test will exercise the basic SVTS services to verify that no problems have developed as a result of the compilation and link. Also, as part of the test, file comparison command will be used on all executable files, data files and script command files to verify that no differences in the applications software exists between the Test Release and the Formal Release. The test will be witnessed and approved by Government representatives.

3.8.5.3 Test Failures and Recovery for Post Release Tests.

3.8.5.3.1 Detection/Correction Of Errors. If the Post-Release Test has a software related failure, the failure will be investigated. The Government will determine whether to restart the formal compile or to return to the Test Release phase.

3.8.5.3.2 Identification of Work-around/Recovery. Should a failure occur during the Post-Release phase, the Government and the contractor will determine if the problem can be resolved through a work-around. If a failure occurs in the software, but does not prevent the basic operation of the SVTS system or cause major system failure, the contractor, with Government approval, shall open a STR for the problem and fix it in a future software release. If the Government determines that the work-around solution is unacceptable, then the release cycle will return to the Test Release phase.

3.8.6 Field Test. The field test is conducted as part of software installation. See section 3.10.3.

3.9 **File Management**. A software source code control applications (currently DEC Code Management System (CMS) will be used to manage system files and libraries. The contractor shall manage system files in accordance with the procedures of section 3.9, the procedures of the Programmer's Maintenance Manual (minus STR management and Discrepancy Reports), the Software Installation Manual, the contractor's approved Software Development Plan, and the contractor=s approved Configuration Management Plan.

3.9.1 Holding Library.

3.9.1.1 Library Description. During the software development cycle of a software build, the contractor shall establish and maintain a holding library, (currently called D ark), to control access to the files being modified during the development. When the development is complete and the approval cycle successfully met, the software modules from the holding library will be promoted to the release library. During the development cycle the holding library is used to create a controlled directory location for the newly modified or created modules. Using the Code Management System and contractor generated command files, will assure the following controls on modules being modified for a build:

(1) Only one engineer at a time can reserve (modify) a module.

(2) All modules associated with a change subtask/STR will

be placed into a common group. This differentiates multiple changes to the same module.

(3) When a module is replaced into the holding library, the engineer and CM will be supplied with the SLOC count of the module before and after the change and the code differences between the old and new version of the module. These differences also supply another level of checking to assure that changes are not lost.

(4) When a test compile is generated, the user will be prompted for a list of subtask/STRs (changes) to include into the compile.

3.9.1.2 Interim Release Procedures. If during the development cycle of the next software release, an emergency software change (STR/Subtask) to the current release must be installed in the field, the following procedure shall be used to produce an interim release:

A new holding library will be generated so that the modules affected by the emergency STR/Subtask can be isolated from the software modules currently under development for the next release. The affected modules will be fetched from the current CMS release library. As changes are made, the modules are returned to the new library. Since a separate holding library is being used to support the emergency STR/Subtask, the software effort for the interim release and the next release can continue concurrently without interfering with each other. The system compilation is executed using the new library and the CM baseline software. Since the modules under development for the next release have not been promoted and are located in a separate holding library, the interim release contains the current CM baseline software and the updates to resolve the emergency STR/Subtask only. After the interim release has been validated for installation to the field, the affected modules are promoted to the CM baseline software. Modules that were changed for the interim release and also are currently being developed for the next release shall be manually validated by the contractor to insure that the interim release changes are included in the software for the next release. The Individual Regression Test plans executed, the interim build will also be included in testing associated with the next release.

3.10 **Software Installation**.

3.10.1 Overview. The installation process has three main objectives. First, the installation must be accomplished in a

manner that will ensure minimum disruption to the existing operational system. Second, the installation process must be rigidly controlled to reduce risks associated with certification of the new release. Finally, the CHECKSUM program must be run without impairing the operational system for long periods and should verify the validity of the software installed onto the system. Software shall be installed on the system in accordance with section 3.10, the SVTS Software Installation Manual, and the contractor developed and Government approved procedures in the Software Development Plan and Configuration Management Plan.

3.10.2 Software Loading Procedure. For each release, the contractor shall prepare, in the DE&I facility, two sets of installation disk packs. One set will be under CM control and kept in the DE&I facility; the other will be kept at the Hub. The primary installation disk packs, created in the DE&I facility, will be used to initially load the new release. For procedures on loading software onto the SVTS system, refer to the SVTS Software Installation Manual.

3.10.3 Field Test

3.10.3.1 Purpose of Test. After the new release is installed in the field the field test (minimum service checkout and broadcast) will validate the basic functionality of the installed release. The test shall be written using CDRL S008 and is due for Government review two weeks prior to conducting the test. The Government will have one week to review the Field Test Plan. The contractor shall correct any changes recommended by the Govern- ment within one week of the review. The test will be witnessed and approved by Government representatives.

3.10.3.2 Description of Test. The test will exercise the basic SVTS services to verify normal functioning of the release. As a minimum, the field test will consist of a six-site FMV call and six-site MLVT call. It shall include the addition and dele- tion of sites. Specifically, it will test those functions in the System Regression Test plan that require more than three nodes. The duration of the test should be kept to a minimum to minimize system down time. The contractor shall provide personnel at the test sites and Hub in order to conduct the test.

Should a failure occur during the field testing, the Government will determine if the problem prevents basic operation of the SVTS system. If the determination is made that the Formal Release prevents the basic operation of the SVTS system, the previous release will be reinstalled at all sites, and the testing cycle will return to a point in the Test Release phase as

determined by the Government to be appropriate.

3.10.4 Documentation. One week after successful installation and testing of the software in the field, a Version Description Document (CDRL S003) and a test report shall be submitted to the Government for approval. The test report will include a brief description of the task, test preparation, test performance, test results, and all the recorded comments made during the testing. The Software Test Report format is documented in CDRL S009. The Government will have two weeks to review the documentation. The contractor shall have two weeks to update the documentation based on Government recommendations from the review.

ANNEX A
SECURE VIDEO TELECONFERENCING SYSTEM
CHANGE PROPOSAL FORMAT

ITEMS 1-16 ARE TO BE COMPLETED BY THE ORIGINATOR

1. System Name - Enter the name of the system to which this report applies.

2. Title of Change - Enter a brief descriptive title indicating the purpose of the change.

3. Change Proposal Number - Use consecutive change proposal numbers beginning with the site number, type of change, calendar year, and site-specific sequence number (e.g., Site 2-ECP-87-1). (The same change number will be used for subsequent submission of the same change proposal.)

4. Type of Change - Enter type of change: Engineering Change Proposal (ECP) or Software Change Proposal (SCP)

5. Change Classification (for ECPs only) - Enter the name of the organization initiating the proposal.

6. Originating Organization - Enter the name of the organization initiating the proposal.

7. Originator - Enter the name, address, telephone number, and title of the individual submitting the proposal (originator's signature must appear in the signature block at the end of the submitted change proposal.)

8. Priority of Change - Enter priority of change (i.e., Emergency, Urgent, or Routine).

9. Description of Change - Enter a description of the proposed change in detail sufficient to permit ready identification and evaluation. Indicate whether the impact of the change warrants the issuance of a new version of the software Configuration Item (CI).

10. Description of Need for Change - Enter a comprehensive description of the need or new capability the proposed change intends to provide and include the justification for approving the change.

11. Recommended Solution - Provide the advantages and

disadvantages of the various solutions considered and an analysis showing reasons for adopting the solution recommended, including an assessment of the impact if no solution is implemented. Enter a detailed description of the recommended solution.

12. Impact Analysis - Describe the cost, schedule, and interface impacts if the solution is approved. Include the impact on other configuration items, integrated logistics support, security, system resources, maintenance, and operations (e.g., manning, training, and procedural considerations.) See appendix B for a detailed checklist of impacts to be assessed. Documentation affected is addressed in item 19 below.

13. Approval Need Date - Enter the date approval is required.

14. Implementing Actions - Enter actions necessary to implement the approved change.

15. Implementing organization - Enter the name of the implementing organization (proposed).

16. Implementor - Enter the name and telephone number of the individual point of contact (proposed) who will be responsible for ensuring the change is implemented correctly.

17. Configuration Item (CI) Nomenclature - Enter the specific CI nomenclature which identifies the CI(s) modified or affected by the proposed change. For hardware CIs, cite the unit number, module name assembly number, and subassembly identifiers. For software CIs, cite the processor (i.e., Node Control Processor, Hub Control Processor, Word Processor) or terminal (i.e., User Control Terminal), the CI component (file name), and version number.

18. Baseline(s) Affected - Enter the name of all established or controlled baseline affected by this proposal (i.e., functional, allocated, or product baseline for Pre-Minimum Critical Services (MCS) Initial Operational Capability (IOC-Manual), MCS (IOC - Automatic), IOC - Enhanced Full operational Capability (FOC).

19. Documentation/Specification Affected - Enter the name and document number for all documentation and drawings that would be affected by this proposal.

20. Approval Authority - Obtain the signature of the CMWG Chairman indicating approval or disapproval by the CMWG. (The Program Manager will ensure that the CMWG Chairman's signature, date, and disposition are reflected in the signature block.)

21. Certifying Authority - Obtain the signature (and date) of Network Certification Working Group (NCWG) representative authorized to certify the site/system. This signature indicates that the site/system is certified for continued operations based on correct implementation and test of the approved change. (As appropriate, the Program Manager will ensure that the certifying authority's signature appears in the signature block.)

22. Signature Block

Submitted by:

(Signature) (Date)

(Originator's typed name and title)

Approved (or disapproved) by:

(Signature) (Date)

SSWG Chairman's typed name and title)

Certified by:*

(Signature) (Date)

(Certifier's typed name and title)

* To be signed/certified by the system certifier only if the proposed change has been approved by the SSWG Chairman.

ANNEX B
IMPACT ANALYSIS CHECKLIST

This appendix provides a checklist for the analysis of impacts of a proposed change. Impact statements will be prepared by the originator and included as item 12 of the proposed change. Impact statements will be considered in the evaluations and technical recommendations of the Principal Action Officer (PAO) and other representatives involved in the change approval process. Items suitable for impact analysis include the following:

a. Costs

(1) Estimated equipment and software costs (development or purchase).

(2) Estimated logistics support costs (include cost of personnel, operator and maintenance training, spares and repair parts for a specified period).

(3) Total estimated cost.

b. Benefits

(1) Quantifiable benefits (in terms of dollars).

(2) Qualitative benefits.

(3) Net cost/benefit relationship.

c. Schedule

(1) Estimated production (development), delivery and installation schedule.

(2) Impacts on phased system development and implementation schedule.

d. Interface

(1) Other systems affected.

(2) Other Configuration Items (CIs) affected.

(3) Effects on performance and functional characteristics of other related systems of CIs.

e. Security - Refer to the checklist provided in the CHOSUN Network Certification Plan.

f. Other

(1) Effects on skills, manning, training, or human engineering design related to the CI to be changed as well as other related systems or CIs.

((2) Effects on operational effectiveness. Examples are as follows:

(a) Required changes to data base parameters, values, or data base management procedures.

(b) Estimated effects on program execution time.

(c) Estimated net effect on availability of excess memory.

(d) Other relevant impacts on utilization of computer resources.

(3) Effects on the system development program. Examples are as follows:

(a) Effects on computer program redesign, testing, installation and checkout.

(b) Effects on system components still under development.

(4) Effects on integrated logistic support elements. Examples are as follows:

(a) Spares and repair parts that are changed, modified, or obsolete.

(b) Maintenance concept and maintenance training requirements in terms of training equipment, trainers, and training programs for operator and maintenance courses.

(c) New, revised, obsolete, or additional test support equipment and test procedures.

ANNEX C
SOFTWARE TROUBLE REPORT PREPARATION INSTRUCTIONS

BLOCK/TITLE PREPARATION INSTRUCTIONS

a. Date. The date form is prepared (MM/DD/YY).

b. Category. Circle an appropriate category (S, D, E, or L):

Software Trouble (S): The software does not operate according to supporting documentation and the documentation is correct.

Documentation Trouble (D): The software does not operate according to supporting documentation but the software operation is correct.

Design Trouble (E): The software operates according to supporting documentation but a design deficiency exists. The design deficiency may not always result in a directly observable operational symptom but possesses the potential of creating trouble.

Logic Trouble (L)

c. Priority. Circle appropriate priority (1 through 5):

(1) Error which prevents the accomplishment of an operational or mission essential function in accordance with official requirements (e.g., causes a program stop, or Hub switch shut down or failure, HCP crash) which prevents the operator's accomplishment of an operational or mission essential function, or jeopardizes personnel safety.

(2) Error which affects the accomplishment of an operational or mission essential function in accordance with official requirements for which no alternative work-around solution exists; or which adversely affects the operator's accomplishment of an operational or mission essential function so as to degrade performance and for which no alternative work-around solution exists. (Note: Reloading or restarting the software is not an acceptable work-around solution.)

(3) Error which affects the accomplishment of an operational or mission essential function in accordance with official requirements for which there is a reasonable alternative work-around solution; of which adversely affects the operator's

accomplishment of an operational or mission essential function so as to degrade performance and for which there is a reasonable alternative work-around solution. (See note under priority 2).

(4) Error which is an operator inconvenience or annoyance and does not affect a required operational or mission essential function.

(5) All other errors.

d. STR Number. Filled in by System Software Configuration Management.

e. Title. Enter a brief, but concise description of problem.

f. Related STR number. (if applicable)

g. Unit/Site. Enter unit or test site at which trouble was detected.

h. Reference Document. Enter official designation of document which provides the basis for determining a trouble exists.

i. Function Affected. Identify the operational function of the component affected by the trouble: HCP, NCP, UCT, or others.

j. Responsible Module(s). Identify the component to which the programmer isolated the problem and complete identification of the component, version, date, and any other significant component identification data.

k. Originator. Enter printed name of individual originating report.

1. Detection by. Identify the problem by:

(1) User

(2) Program office

(3) Hub Controller

(4) Maintenance personnel

(5) Contractor's software team

(6) Contractor's hardware team

m. Tel/Ext. Enter telephone number of individual originating report.

n. Run Time. Enter the elapsed time (in hours/quarter hours) from program start until trouble occurred.

o. Simulation. Enter program equipments used to simulate operational conditions. Indicate tape reel number, if applicable.

p. Problem Duplicated. Check (as applicable) duplication attempts/success/failures for software troubles.

| | YES | NO | NA |
|---|---|---|---|
| (1) During run | | | |
| (2) New software | | | |
| (3) After restart | | | |
| (4) After reload | | | |

q. System Status. Delineate any particular system/subsystem equipment states necessary to properly describe to system environment at the occurrence of the trouble that is not adequately covered by previous blocks (e.g, alternate modes or special operations being conducted, etc.)

r. Technical Description of Approach. Describe the proposed solutions for the specified processor and identify the images/ modules affected. Explain all assumptions made in generating the solution, and the limitations imposed on the system by the solution.

s. Unit Modified/SLOC Change. Identify all modules modified and the number of Source Lines of Code (SLOC) affected/changed for each module.

t. Trouble Description. Write sentence defining the trouble, then develop a word picture of the events leading up to, and coincident with, the problem. Structure your statement in order that the programmer/test analyst can duplicate the situation. Cite equipment being used, an unusual configuration, etc. if applicable, also indicates consoles on line, modes, etc. Use continuation sheets, whenever required and fill in the page. of at the top of the STR form; attach the continuation sheet(s) to the STR form.

u. STR Status. Enter the appropriate STR status/disposition code number to indicate the current status of the STR. When the status changes, enter the new status code number. Status code numbers are as follows:

1X - Under Investigation

11 - Under investigation

12 - Under Investigation, work around exists

13 - Software and Documentation problem

14 - Software problem

15 - Documentation Problem

16 - Previous software corrective action failed retest.

17 - New Enhancement

2X - Problem corrected, complete update not available.

21 - Source code corrected but requires inspection, test, and verification; documentation updated but requires verifications.

22 - Source code corrected but requires inspection, test, and verification.

23 - Documentation updated but requires verification.

24 - Patch applied, a source code and documentation update required.

25 - Patch available but not installed.

3X - Closed/Fixed

31 - Corrected in source code and verified object code available, documentation updated and verified.

32 - Corrected in source code and verified object code available.

33 - Documentation updated and verified.

34 - Patched - correction applied in field, awaiting

official release.

35 - Not repeatable, reported to STR submitter.

36 - Invalid report of software trouble, reported to STR submitter.

37 - Out-of-scope, reported to STR submitter.

38 - Information only

39 - Corrected source code in operation

4x - Misc.

41 - Closed - Hardware fix corrected the problem.

42 - Closed - User misunderstanding of system operation - no software change

43 - Open - awaiting hardware to test hardware related fix.

44 - Closed - Closed with DISA concurrence due to age of STR and inability to reproduce or detect further problems.

45 - Problem resolved with procedural change.

v. Date STR status change. Enter a date to indicate current status of STR (MM/DD/YY).

w. Date implemented. Enter date STR is implemented (MM/DD/YY).

z. OA sign-off. A signature by designated quality assurance (QA) Government representative authorizing implementation of the corrective change(s) and certifying the correctness and completeness of the change(s).

ANNEX D
REFERENCES

MIL-STD-498 Software Development and Documentation
MIL-STD-973, Configuration Management
Network Controller Manual (S)
Node Operator Manual (S), 24 April 92
Programmer's Maintenance Manual; 1 April 1988
Secure Video Teleconferencing System Network Security Officer's Security Guide (S), 15 March 1989
Software Installation Manual (IOC-A), Final, Rev C, 20 FEB 90 (S)
Software Program Specifications, User Control Terminal (UCT), 1 OCT 91 (
Software Program Specifications, Hub Control Processor (HCP), VOL I of II, 1 OCT 91 (S)
Software Program Specifications, Hub Control Processor (HCP), VOL II of II, 1 OCT 91 (S)
Software Program Specifications, Node Control Processor (NCP), 1 OCT 91 (S)
Software Program Specifications, Data and System Utilities, 1 OCT 91 (S)
System Controller Manual (S), 20 May 92
System Interface Specifications, VOL I (Sections 1.0 - 3.0: Introduction, External Interfaces, Inter-Segment Interfaces), 26 JUN 86 w/ REV D, 12 NOV 87 (U)
System Interface Specifications, VOL II (Section 4.0: Hub Inter-Element Interfaces), 26 JUN 86 (U)
System Interface Specifications, VOL III (Section 5.0: Node Inter-Element Interfaces), 23 MAR 88, (S)
System Interface Specifications, VOL IV (Section 6.0: Communications segment Inter-Element Interfaces), 26 JUN 86 (U)
System Interface Specifications, VOL V (Section 7.0: ManMachine Interfaces), 12 OCT 90 (S)
System Summary Report, 16 MAY 86 (S)
SVTS Functional Elements & Component Flow Chart
SVTS Network Security Manual (S)
SVTS Technical Manual (S)
Technical controller Manual (S)

ANNEX E
ABBREVIATIONS

| | |
|---|---|
| CCB | Configuration Control Board |
| CDRL | Contract Data Requirements List |
| CI | Configuration Item |
| CM | Configuration Management |
| CMS | Digital Equipment Corporation's Code Management System |
| CMWG | Crisis Management Working Group |
| COTS | Commerical off-the-Shelf |
| DEC | Digital Equipment Corporation |
| DE&I | Design Engineering and Integration Labratory |
| DISA | Defense Information System Agency |
| ECP | Engineering change Proposal |
| HISSO | Hub Information System Security officer |
| IFS | System Interface Specification |
| NCWG | Network Certification Working Group |
| NISSO | Node Information System Security Officer |
| NSA | National Security Agency |
| NSO | Network Security Officer |
| PAO | Principal Action Officer |
| PMO | Program Management Office |
| SCN | Specification Change Notice |
| SCP | Software Change Proposal |
| SDF | Software Development Facility/Software Development Folder |
| SSWG | Situation Support Working Group |
| STR | Software Trouble Report |
| SVTS | Secure Video Teleconferencing System |